



***Cabinet for Health and Family Services (CHFS)  
Information Technology (IT) Policy***



**065.014 Cabinet for Health and Family Services  
(CHFS) System Development Life Cycle (SDLC) and  
New Application Development**


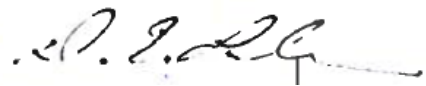
**Version 2.3  
April 16, 2018**

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

## Revision History

| Date      | Version | Description    | Author                        |
|-----------|---------|----------------|-------------------------------|
| 7/20/2010 | 1.0     | Effective Date | CHFS OATS Policy Charter Team |
| 4/16/2018 | 2.3     | Revision Date  | CHFS OATS Policy Charter Team |
| 4/16/2018 | 2.3     | Review Date    | CHFS OATS Policy Charter Team |

## Sign-Off

| Sign-off Level                                  | Date      | Name             | Signature  |
|---|-----------|------------------|--|
| CHFS IT Executive<br>(or designee)              | 4/16/2018 | Jennifer L. Harp |  |
| CHFS Chief<br>Security Officer<br>(or designee) | 4/16/2018 | DENNIS E. LEBER  |  |

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

## Table of Contents

|   |          |
|---|----------|
| <b>065.014 CHFS SDLC AND NEW APPLICATION DEVELOPMENT .....</b>                        | <b>5</b> |
| <b>1 POLICY OVERVIEW.....</b>   | <b>5</b> |
| 1.1 PURPOSE .....   | 5        |
| 1.2 SCOPE .....   | 5        |
| 1.3 MANAGEMENT COMMITMENT.....  | 5        |
| 1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES .....                                  | 5        |
| 1.5 COMPLIANCE .....  | 6        |
| <b>2 ROLES AND RESPONSIBILITIES .....</b>   | <b>6</b> |
| 2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) .....                                   | 6        |
| 2.2 SECURITY/PRIVACY LEAD .....   | 6        |
| 2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER ..... | 6        |
| 2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES .....   | 7        |
| 2.5 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....                             | 7        |
| <b>3 POLICY REQUIREMENTS .....</b>  | <b>7</b> |
| 3.1 GENERAL .....   | 7        |
| 3.2 NEW APPLICATION DEVELOPMENT .....   | 8        |
| <b>4 POLICY MAINTENANCE RESPONSIBILITY .....</b>                                      | <b>8</b> |
| <b>5 POLICY EXCEPTIONS .....</b>  | <b>8</b> |
| <b>6 POLICY REVIEW CYCLE.....</b>   | <b>8</b> |
| <b>7 POLICY REFERENCES .....</b>  | <b>8</b> |

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

## Policy Definitions

- **Application:** A software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Critical Systems:** Any system or application that is federally mandated/regulated, deemed critical by the data or system owner(s), or deemed a “24 hours, 7 days a week, 365 days a year” (24x7x365) application, will be defined as a critical system. CHFS ITMP will be the source of knowledge and repository of severity level for systems/applications.
- **Database (server or components):** A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
- **Oversight Group:** CHFS comprised group including agency and technical staff that will be a part of communication and movement throughout the System Development Life Cycle (SDLC) process.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver’s license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **Web Server:** A computer that runs a Web site. Using the Hypertext Transfer Protocol (HTTP), the Web server delivers Web pages to browsers as well as other data files to Web-based applications (e.g., Internet Information Server (IIS), or Apache).

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

# **065.014 Cabinet for Health and Family Services (CHFS) System Development Life Cycle (SDLC) and New Application Development**

Category: 065.000 Application Development

## **1 Policy Overview**

### **1.1 Purpose**

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a system development lifecycle. This document establishes the Cabinet's System Development Life Cycle (SDLC) and New Application Development Policy which helps manage risks and provides guidelines for security best practices regarding software development, and supporting infrastructure that enables projects delivered within schedule, meet compliance regulations, and reduce overall risk to the Confidentiality, Integrity, and Availability (CIA) of Data systems.

### **1.2 Scope**

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

### **1.3 Management Commitment**

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

### **1.4 Coordination among Organizational Entities**

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

## **1.5 Compliance**

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

## **2 Roles and Responsibilities**

### **2.1 Chief Information Security Officer (CISO)**

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

### **2.2 Security/Privacy Lead**

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

### **2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer**

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

## **2.4 CHFS Staff and Contractor Employees**

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

## **2.5 System Data Owner and System Data Administrators**

It is the responsibility of these management/lead positions, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

# **3 Policy Requirements**

## **3.1 General**

This policy is established to refine uniform business processes and standards to assure quality development projects are delivered on time and within budget.

Each system or group of related systems will define a methodology for managing Software Development Life Cycle (SDLC). The methodology will consist of the following phases, but is not limited to:

- Initiation
- Development
- Testing
- User Acceptance testing (UAT)
- Implementation
- Maintenance and Operations (M&O)
- Decommissioning

CHFS projects shall use the TFS, or agency other approved system(s), to check code in and out during development or for use in production when required. The IS Team recommends that the code be digitally-signed to maintain integrity between development, integration, test, and production environments.

Each system or group of systems will have an oversight group who will have the responsibility of managing projects and changes in accordance with the SDLC methodology.



|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

Per Enterprise Policy- CIO-082 Critical Systems Vulnerability Assessments Policy, each agency shall engage a third party to assess all critical systems under the agency's responsibility both upon initial implementation into production use and at least every two (2) years thereafter.

These network and server vulnerability assessments do not include the development environments, or application software, related to these systems, which must be tested separately. Each agency shall follow the appropriate notification process outlined in the CHFS Systems Development Lifecycle (SDLC) Procedure prior to conducting these assessments.

### **3.2 New Application Development**

OATS requires all new application development efforts to be reviewed and analyzed. Refer to the CHFS Systems Development Lifecycle (SDLC) Procedure for detailed steps when developing new applications.

## **4 Policy Maintenance Responsibility**

The OATS IS Team is responsible for the maintenance of this policy.

## **5 Policy Exceptions**

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

## **6 Policy Review Cycle**

This policy is reviewed at least once annually, and revised on an as needed basis.

## **7 Policy References**

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Systems Development Lifecycle (SDLC) Procedure
- COT Enterprise Architecture and Kentucky Information Technology Standards (KITS) Library
- Enterprise IT Form: Modification Request Form, COT-F026 Form
- Enterprise IT Form: Exception Request Form, COT-F027 Form
- Enterprise IT Form: Security Exemption Request Form, COT-F085 Form
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy



|   |                         |
|---|-------------------------|
| 065.014 CHFS SDLC and New Application Development | Current Version: 2.3    |
| 065.000 Application Development                   | Review Date: 04/16/2018 |

- Health Insurance Portability and Accountability Act of 1996 (HIPAA):
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45CFR164.308(a)(1)(ii)(A)
- Internal Revenue Services (IRS) Publications 1075
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National institute of Standards and Technology (NIST) Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Social Security Administration (SSA) Security Information